1. What is LFI

Local File Inclusion (LFI) is a type of web vulnerability that allows an attacker to access and include files on the web server through the web browser. This typically happens when a web application dynamically includes files based on user input without proper validation or sanitization.

How LFI Works:

- LFI occurs when a vulnerable application allows user-supplied input to specify a file path.
- If not properly filtered, an attacker can manipulate the file path to include files stored on the server, like sensitive configuration files (`/etc/passwd` on Linux) or source code files, which may contain valuable information or lead to further exploitation.

Potential Risks of LFI:

- **Sensitive File Disclosure**: Attackers can read files that contain sensitive data.
- **Code Execution**: In some cases, attackers may be able to execute code from files on the server, leading to full system compromise.
- **Path Traversal**: Attackers can use directory traversal (`../../`) to navigate to directories outside the intended location.

Example of LFI Vulnerable Code:

```php
<?php
  $file = $_GET['page'];
  include($file);
?>
```

Here, if `page` parameter is not validated, an attacker could enter a path like `../../etc/passwd` to read the password file on a Unix system.